SSO Konfiguration

Definition

Menüaufruf: (Administration) - (SSO Konfiguration)

Nuclos unterstützt die Authentifizierung mittels OAuth2 und OpenID Connect (OIDC), und setzt dabei auf den Authorization Code Grant.

Client-Login

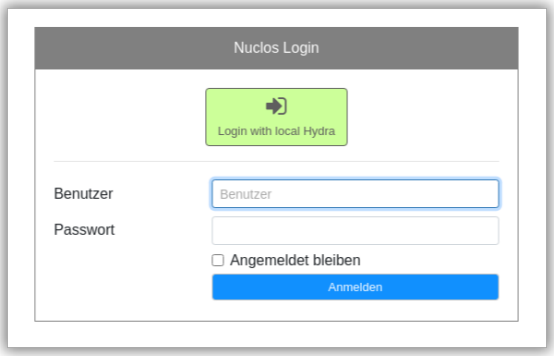
Aktive Dienste werden den Endbenutzern zur Authentifizierung beim Starten eines Clients angeboten.

Rich-Client

Der Rich-Client verwendet den Webclient mit. Der Login Button, in diesem Beispiel "Login with local Hydra", öffnet also den Browser und leitet den Benutzer durch den Authentifizierungsprozess, falls noch keine Sitzung vorliegt. Im Anschluss wird der Nuclos Webclient geöffnet und autorisiert durch diesen letzten Schritt auch den Rich-Client. Dieser startet in Folge dessen und der Webclient zeigt eine Bestätigung.

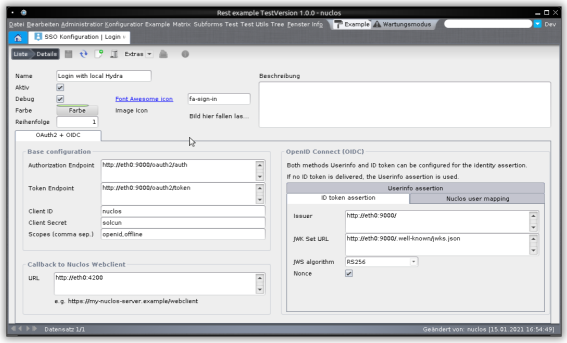
Webclient

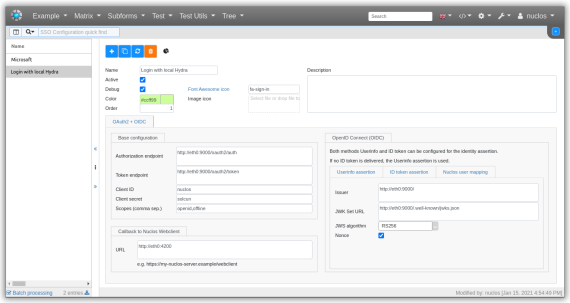
Auch in diesem Beispiel wird mit dem Login Button "Login with local Hydra" der Authentifizierungsprozess gestartet.



Konfiguration

Die Konfiguration der zur Verfügung stehenden SSO Dienste erfolgt innerhalb eines Clients, zu finden im Menü Administration.





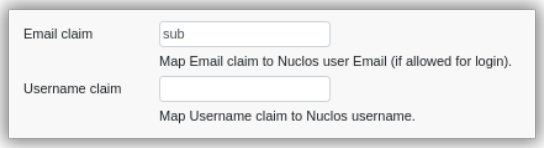
Callback to Nuclos Webclient

Für die Callback URL zum Nuclos Webclient ist immer der ROOT Pfad des Webclients anzugeben, mit der ein Browser eines Endbenutzers den Webclient auch tatsächlich erreichen kann. Sollte z.B. ein Load Balancer zum Einsatz kommen, oder ein Reverse Proxy o.ä. ist das zu berücksichtigen. Für eine typische Installation mit dem Nuclos Installer wäre es z.B. *https://my-nuclos-server.example/webclient*

OAuth2 Konfiguration

Die nötigen Einstellungen sollte Ihnen Ihr SSO Anbieter nennen können. Nicht immer sind alle Felder zu füllen. Zum testen der Einstellungen kann ein "Debug" eingeschaltet werden, womit Log Ausgaben zum SSO Authentifizierungsversuch vom Nuclos Server im server.log ausgegeben werden.

OIDC Abfrage der Benutzerinformationen



Die Ermittlung der Benutzerinformationen über OIDC erfolgt entweder über ein ID Token oder einen Userinfo Endpunkt (weiterer Request). Ein ID Token bietet in der Regel mehr Sicherheit und wird daher vorrangig verwendet. Hierzu müssen im Reiter **ID token assertion** die nötigen Einstellungen erfasst werden. Fehlt die "Issuer" Einstellung oder wird kein ID Token geliefert, so wird der unter **Userinfo assertion** konfigurierte Endpunkt zur Ermittlung des Benutzers angefragt.

In beiden Fällen erhalten wir ein ClaimsSet (Beispiel aus dem Log: {"sub":"foo@bar.com","sid":"1bddcca8-bfbc-487c-a9d6-80f60e7e658d"}) in dem entweder die E-Mail Adresse oder der Benutername des **Nuclos** Benutzers enthalten sein muss, um die Authentifizierung Nuclos-seitig abzuschließen. Um die Ermittlung möglichst flexibel zu gestalten kann im Reiter **Nuclos user mapping** das Attribut des ClaimsSets hinterlegt werden. Die Suche über die E-Mail erfolgt zu erst, bleibt diese erfolglos wird noch eine Suche über den Benutzernamen versucht, falls konfiguriert. Eines von beidem muss also zwingend konfiguriert sein.

> **Email Suche**
>
> Achtung, für eine erfolgreiche Ermittlung über die E-Mail Adresse ist das Flag **Login mit E-Mail Adresse zulassen** am Benutzer eine Voraussetzung!

Hintergrundinformationen

Requests & Sitzungsdauer

Der OAuth2 Dienst wird zusätzlich zur anfänglichen Authentifizierung auch zur Erneurung der Refresh Tokens in regelmäßigen Abständen (bei Ablauf eines Tokens) angefragt, sofern vom Dienst bei der Anmeldung mitgeliefert. Werden keine geliefert, oder ist die Erneurung erfolglos wird der Benutzer ausgeloggt. Ein Richclient schließt sich nach Meldung der abgelaufenen Sitzung komplett. Da so womöglich ungespeicherte Änderungen verloren gehen, sollte möglichst der OAuth2 Dienst Refresh Tokens zur Verfügung stellen.

Für unseren Nuclos Server ist auch weiterhin die JSESSIONID (Cookie) ausschlaggebend und wird bei jedem Request geprüft. Ein OAuth2 Dienst wird damit möglichst wenig beansprucht.

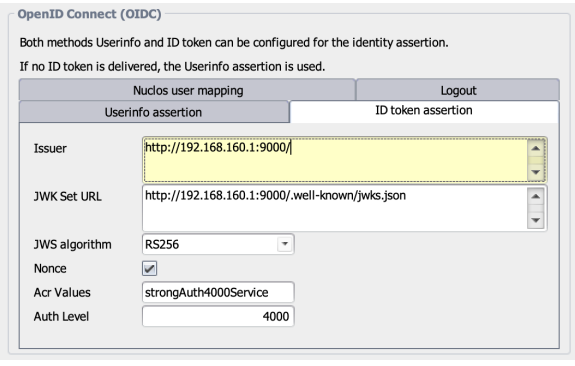
Logout

Ein Logout in Nuclos hat bisher noch keine Auswirkungen auf den OAuth2 Dienst, wird also (noch) nicht weitergeleitet, es wird lediglich die Nuclos Sitzung beendet. Auch wirkt sich ein Logout im OAuth2 Dienst noch nicht direkt auf eine Nuclos Sitzung aus. Nur indirekt, da zu erwarten ist, dass ein Refresh Token nicht erneuert werden kann.

Sticky Sessions (Clustering)

Ein Clustering von Nuclos Application Servern setzt zwangsläufig Sticky Sessions vorraus, da es für eine Sitzung Informationen geben kann, die nur am Application Server abgelegt und nicht unter den Servern ausgetauscht werden. SSO relevante Informationen (Tokens etc.) gehören auch dazu.

Zwei-Faktor Authentifizierung (2-FA)



Parameter acr_values

In vielen Systemen lässt sich mit dem Parameter "acr_values" konfigurieren, welche Möglichkeiten zum Anmeldung erlaubt sind. Daher gibt es ab Nuclos 4.2022.36 in der SSO Konfiguration ein neues Feld "Acr Values":

Im Screenshot wird durch "strongAuth4000Service" eine 2-FA Authentifizierung erzwungen. Dieser einzutragende Wert ist von System zu System unterschiedlich.

Parameter Auth Level

Ab 4.2022.38 kann ein numerischer Wert angegeben werden, der dazu dienen, bestehende Authentifizierung zu überprüfen, ob sie "hoch" genug sind. Damit das überhaupt funktionieren kann, muss der SSO-Server eine bestimmte Response mit Wert zurückgeben. Falls der Wert zu niedrig ist oder die Syntax nicht genau den Erwartungen erfüllt, scheitert die Überprüfung.
Die Implementierung zu "Auth Level" befindet sich noch Beta-Stadium und wird für viele System nicht funktionieren. Daher sollte hier nichts eingetragen werden, wenn man nicht die Kompatibilität kennt und/oder es Probleme gibt.